(7)

MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2022/2023 (TERM ID 2210)

ECE3256 CYBERSECURITY

(All Sections / Groups)

7 FEBRUARY 2023
9:00 A.M – 11:00 A.M.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 8 printed pages including the cover page with 4 questions only.

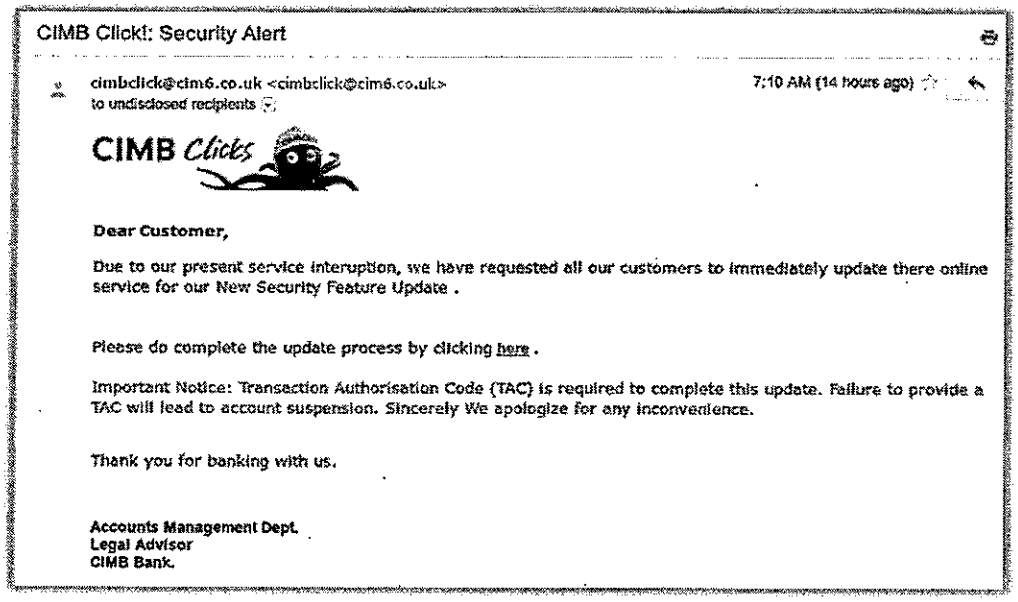
2. Attempt all FOUR (4) questions. All questions carry equal marks and the distribution of marks is given in the questions.

3. Please print all your answers in the answer booklet provided.

4. State all assumptions clearly.

Question 1

(a) You received an urgent email out of the blue from a bank as shown in Figure Q1(a).


CIMB Click!: Security Alert

cimbclick@cim6.co.uk <cimbclick@cim6.co.uk> 7:10 AM (14 hours ago)
to undisclosed recipients

CIMB Clicks

Dear Customer,

Due to our present service interuption, we have requested all our customers to immediately update there online service for our New Security Feature Update .

Please do complete the update process by clicking here .

Important Notice: Transaction Authorisation Code (TAC) is required to complete this update. Failure to provide a TAC will lead to account suspension. Sincerely We apologize for any inconvenience.

Thank you for banking with us.

Accounts Management Dept.
Legal Advisor
CIMB Bank.

Figure Q1(a)

(i) You suspect it is a phishing email. What are the signs or indicators that revealed this email to be a phishing email? Describe at least **THREE (3)** signs.

[6 marks]

(ii) If are in doubt of the legitimacy of this email, what can you do to confirm its validity?

[1 mark]

(b) List **THREE (3)** goals of cybersecurity. For each of them, give an example in the context of information technology or computing domain.

[6 marks]

(c) Social engineering is a type of cybersecurity attack.

(i) Explain social engineering.

[2 marks]

(ii) List the **FOUR (4)** psychological traits that an attacker can exploit in social engineering.

[4 marks]

Continued...

(iii) There are many known, and even more unknown social engineering scripts or stories that can be used against unsuspecting users. What advice, suggestions, or tips can you give to prevent a social engineering attack?

[3 marks]

(d) What is Defense-in-Depth and provide examples of how each "depth" can be achieved.

[3 marks]

Continued...

Question 2

(a) Top Security Sdn Bhd is a cybersecurity company that has developed their own cryptography algorithm. They claim that their system is absolutely secure but refuses to disclose their algorithm for public scrutiny because it will supposedly weaken the security. How does this scenario relate to *Kerckhoff's Principle*?

[2 marks]

(b) The Multiplicative Cipher is a type of monoalphabetic cipher.

(i) Write the **corresponding decryption formula** if the encryption formula is written as:

$$C = E(P) = (15 \cdot P) \bmod 26$$

[Note: You do not need to calculate the multiplicative inverse yet.]

[1 mark]

(ii) Explain why $k = 15$ is a suitable key for the multiplicative cipher in Part (i).

[2 marks]

(iii) Calculate the multiplicative inverse of 15 mod 26 using the trial-and-error method. Show all your steps, including the calculations used to obtain the answer.

[3 marks]

(iv) Decrypt the following word using the $k = 15$. Show your steps to decrypt the word.

KECVI

[3 marks]

(c) Using Advanced Encryption Standard (AES), perform the following operations.

(i) Express the following plaintext as an AES state.

Plaintext: {6B C2 BE E2 2E 40 9F 96 E9 3D 7E 11 73 93 17 2A}

[1 mark]

(ii) Assume that the plaintext state in Part (i) is the input into AES' **SubBytes** function. Show the new state after SubBytes using the S-Box in Figure Q2(c).

[3 marks]

Continued...

(iii) Subsequently, show the output state after the **ShiftRows** function is applied on the results of Part (ii).

[3 marks]

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

x

The Substitution Table – Sbox[xy] (in hexadecimal)

Figure Q2(c)

(d) Consider the RSA cryptosystem with $p = 7$, $q = 17$ and $e = 5$.

(i) Find the corresponding decryption key, d using the given parameters.

[3 marks]

(ii) Write down the formulas for encryption and decryption

[2 marks]

(iii) Subsequently, encrypt the message, $m = 4$ using the appropriate formula from Part (ii)

[2 marks]

Continued...

Question 3

(a) After studying the event logs of the company's computers (servers and workstations), you noticed that these computers are systematically **scanned** by an unknown source.

(i) What is the name of this activity?

[1 mark]

(ii) What are the goals or objectives of this activity?

[2 marks]

(iii) Is this a type of active or passive attack? Justify your answer.

[2 marks]

(iv) How can you mitigate this type of activity?

[2 marks]

(b) Describe the following types of active network attacks and **ONE (1)** of their corresponding mitigation methods

(i) URL Spoofing

[3 marks]

(ii) Evil Twin Access Point

[3 marks]

(c) Answer the following questions in relation to an Intrusion Detection System (IDS).

(i) What does IDS stand for in the context of computer security?

[1 mark]

(ii) What does an IDS do?

[3 marks]

(iii) Name and explain the **TWO (2)** categories of IDS based on **what they monitor.**

[4 marks]

(iv) Name and explain the **TWO (2)** categories of IDS based on **how they function.**

[4 marks]

Continued...

Question 4

(a) Briefly explain the following types of viruses or issues related to viruses.

(i) Program virus

[2 marks]

(ii) Boot sector virus

[2 marks]

(iii) Macro virus

[2 marks]

(iv) Stealth and polymorphic virus

[2 marks]

(v) How can a user prevent virus infections? Briefly explain **TWO (2)** methods.

[2 marks]

(b) Ah Seng Sdn Bhd is a small business with a basic website that displays company details, products, location, and other *static* information. The webpage is only updated if there are changes to the product range, which is typically once every 4 months.

Describe a backup strategy that includes the type of backup, frequency of backups, and your justifications.

[3 marks]

(c) Design a layered security strategy to protect the company's computing infrastructure shown in Figure Q4(c). To do this, explain at least **FOUR (4)** tools (e.g. software, devices, policies) that could be used. Your explanation for each of the tool should contain:

(i) A brief description of each tool

[4×1 marks]

(ii) How each tool protects the computing infrastructure

[4×1 marks]

(iii) Where should the tool be placed in the network. Redraw Figure Q4(c) in your answer booklet after the security tool has been properly added.

[4×1 marks]

Continued...

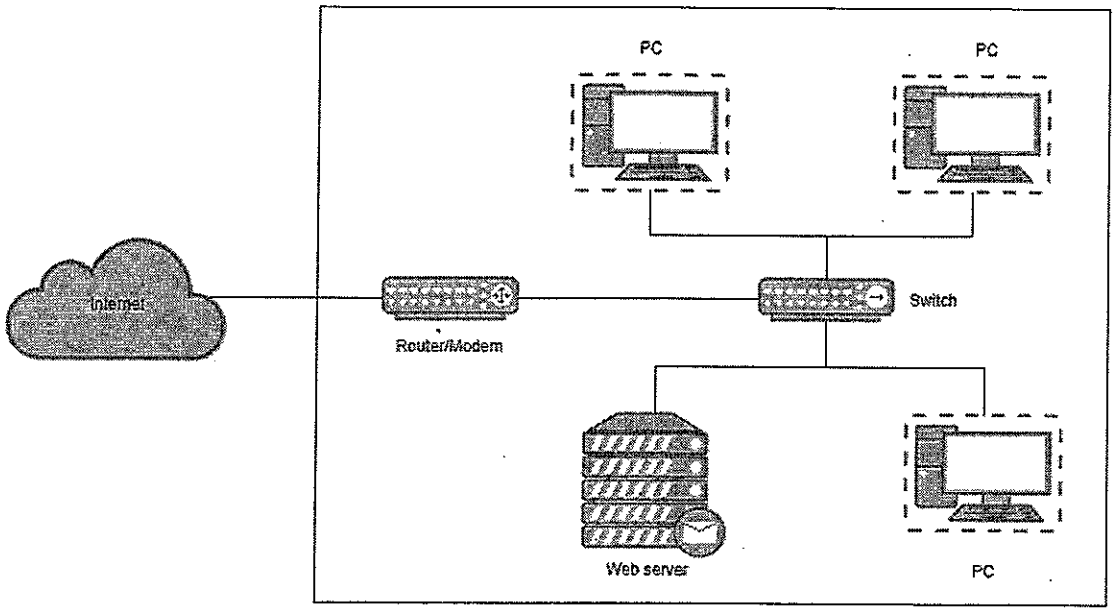


Figure Q4(c)

End of Paper